Submission
Privacy Bill

NZ Council for Civil Liberties
nzccl.org.nz
20th May 2018

About this submission

Oral submission

The NZ Council for Civil Liberties wishes to appear before the committee.

About the submitter

The New Zealand Council for Civil Liberties is a watchdog for rights and freedoms in New Zealand. Formed in 1952, the Council works through education and advocacy to promote a rights-based society and prevent the erosion of civil liberties by government or any other parties. It is a voluntary not-for-profit organisation.

Contact details

Enquiries can be directed to the NZ Council for Civil Liberties' Chairperson, Thomas Beagle, on 021-80-50-40 or at thomas@nzccl.org.nz.

Privacy in 2018

The NZ Council for Civil Liberties has long accepted that privacy is one of our core civil liberties and sees that protecting the privacy of New Zealanders is part of our mission.

Privacy, and the associated control of personal data and how it is used, is vital to a sense of personal autonomy. The feeling of being watched and controlled is antithetical to people having the freedom to make their own choices and live their lives how they wish.

We wish to recognise the part played in New Zealand by the original Privacy Act and the various Privacy Commissioners over the years. This far-sighted Act has been of immense value to New Zealand as the issues around privacy have evolved in the digital age.

That said, we do agree that the Privacy Act does need updating. While written in a technologically neutral way, new circumstances have arisen as digital capabilities have increased and people have thought of new ways to use personal data.

Individual data vs mass invasion of privacy

Not least, personal information is being aggregated and processed so that it can be used to predict behaviour and manipulate people. Combined with certain companies' dominance over access to information, the use of personal data is becoming a threat to our democracy.

Privacy law is no longer just about protecting individuals, but has become an important part of protecting our society. Unfortunately we do not see this reflected in the new Privacy Bill.

The assumption behind the new Bill is that we merely need to protect individuals. However, there are serious problems with this view:

- Large data collection companies can now use information from other people to build up profiles of people who don't participate directly (often called shadow or ghost profiles).
- It doesn't consider the negative societal impact of the multiplier effect where many people give way what is to them inconsequential data but this can be aggregated and used to manipulate and control.

This bill needs to recognise that calculating or deriving personal data from other sources is merely another form of data collection that needs to be covered by the Privacy Principles, including the requirement to be collecting it with permission. And while it is too late for this bill, we believe that some of the wider issues around the use of personal data to manipulate and control people will have to be considered in a future update.

Anonymisation and re-identification

Related to this is the process of re-identifying people in data that has been anonymised. This has proved, time and again, to be far easier than intuition would indicate. This is especially true

when the agency doing the re-identification has access to other data collections that can be cross-referenced. It is often impossible for an agency releasing such data to predict which auxiliary sources of data might become available in future which would enable this for any individual dataset.

Indeed, these days it seems safest to assume that any anonymous data that is rich enough to be useful has already been de-anonymised by data companies such as Facebook.

We therefore ask that the phrase “identifiable individual” be replaced with, simply, “individual” to make clear that in all cases when releasing individual-level private information (or insufficiently aggregated private information) there is potential for individuals to be identifiable. It is therefore always incumbent on agencies to ensure their release of such information is with the meaningful and active consent of the individual (and not just buried in a multi-page privacy policy which no one reads).

Furthermore, we have always read the existing Privacy Act as already covering re-identified data. In our view the data “collection” happens at the point the data is de-anonymised and therefore all of the normal Privacy Act protections apply. In other words, you would need to get the permission of the individual before you could de-anonymise data about them.

It is apparent that others do not share this interpretation or believe that, as this would be impracticable, it should not apply. Therefore we ask that this be explicitly included in the new Privacy Bill, possibly by making it clear that the Privacy Principles, including the need for the permission of the person, apply to personal data collected or generated in this way.

Finally, we note that it may be necessary to provide some form of protection from such laws for bona fide researchers acting in good faith to further the cause of privacy and data security.

Privacy policies and customer agreements

While the Privacy Act was far-sighted in many ways, the authors apparently did not foresee the wide use of unavoidable commercial contracts and privacy agreements that allow agencies to capture and use data as they see fit with the ‘agreement’ of their customer. This situation is particularly unfortunate when the providers are dominant in their markets (e.g the 2-4 phone providers, the banks, local public transport companies) and consumers have little choice but to agree.

We recommend that such wide-ranging “do what you like” agreements be banned. Any mandatory privacy agreement must only cover the bare minimum of information and sharing required to provide the good or service.

Additional collection or sharing of data should be covered by separate agreements that must be done with the meaningful and active consent of the individual concerned, with no penalty or refusal of service to those who do not participate. Furthermore, any agency wishing to use this must also provide a way for individuals to revoke such access at any time in the future.

Law enforcement access to data

The NZ Police have long relied on the “maintenance of law” exception to request and access private data. Some companies, including significant holders of private information such as banks, appear to have got into the habit of giving the NZ Police whatever data they want, ignoring their own responsibility to their customers.

We welcomed the Privacy Commissioner’s decision on this issue in 2017 which interpreted the Privacy Act to say that particularly personal data should generally not be handed over without the Police having an appropriate legal authority requiring it. We recommend that this interpretation should be explicitly added to the Privacy Bill.

Spy agency access to data

The Council believes that law enforcement and security services should be held to higher standards than other agencies. By proposing the opposite this bill threatens to erode the public confidence that these agencies need in order to function. To this end, the Council proposes removing 19(IPP4)(b) and 19(IPP10)(2), and replacing 25 in its entirety with:

> The following government agencies may choose not to comply with IPP 2, 3, and 10 when they can establish a reasonable belief that there exists a specific, serious threat to public safety and that:
>
> (1) The private information being collected contains evidence material to this specific threat;
> (2) Compliance with the IPPs would materially increase the specific threat to public safety; and that
> (3) The extent to which the IPPs are being avoided is proportional to the specific threat.
> (4) This clause can only be enacted by:
>
> i) New Zealand Police
> ii) New Zealand Defence Force
> iii) Intelligence and security agencies

Complaints re intelligence agencies

The procedures around handling reports generated from complaints leave too much up to discretion and fail to involve the appropriate watchdog agency, the Inspector General of Intelligence & Security.

We recommend that:

1. Any report given to an intelligence agency under section 100(2) should also be given to the office of the Inspector General of Intelligence & Security.
2. In section 100(5), change “the Commissioner may send a copy of the report to the Prime Minister” to “the Commissioner must send a copy of the report to the Prime Minister“.

3. In section 100(6), change “the Prime Minister may present the report, or any part of the report, to the House of Representatives to “the Prime Minister must present the report, or any part of the report, to the House of Representatives.”

Automated decision making

Immigration New Zealand was widely and strongly condemned in April 2018 for its inappropriate application of automated decision making based on profiling of individuals. From the strength of this condemnation, it is clear that the people of New Zealand are in favour of strengthening legal limits on automated decision making. The European Union’s General Data Protection Regulation (GDPR) article 22 provides a clear legal framework limiting inappropriate use of “big data”.

The Council recommends adding an IPP 13, worded in line with the GDPR:

> **Information Privacy Principle 13**
> *Automated profiling not to be applied to adjudication of individual cases*
> An agency that holds private information must not subject any specific individual to a decision based solely on automated processing, including profiling, which significantly affects that individual alone.

Penalties

We approve of the new penalties regime for breaches of the Privacy Act. Laws without consequence can and will be ignored by those without conscience.

We are concerned that the penalties may not be sufficient to discourage large companies from breaching the Act, and recommend that the maximum penalties for organisations be raised significantly.

We also note that the European Court of Justice has the option of daily penalties that can be imposed until such time as a company complies with the law. We believe that this should be added as an available option to the new Privacy Act.

Information sharing agreements

As well as being published by the lead agency, we believe it would be advantageous for all information sharing agreements established under part 7 of the Bill to be collated and published online by the Privacy Commissioner. This will allow people to consider the overall scope of information sharing agreements, and locate agreements from agencies that they might not otherwise be aware of.

This could be added as a requirement as a new section in 144(4).

Office of the Privacy Commissioner and the Official Information Act

We consider that this Bill continues to grant the Privacy Commissioner an overly broad exemption from the Official Information Act.

Section 116 has been re-enacted as section 206 without significant changes. This section requires secrecy (206(1)) but grants the Privacy Commissioner the option to disclose information at his or her discretion (206(2)). This presumption of secrecy is the inverse of open, transparent government and the spirit of the Official Information Act: that government-held information should be made available unless there is good reason to withhold it.

We ask that section 206 be removed from the Bill, with secrecy where required (such as of investigations) achieved by instead relying on the extensive withholding grounds available under the Official Information Act - such as legal privilege, and maintenance of the law.

Exclusion of the Ombudsman

We note that the Bill continues to exclude the Ombudsman from its definition of 'agency' in section 6(b)(ix). We ask that this exclusion be removed, as was recommended by the Law Commission (recommendation 37). We have not been able to find any explanation why this recommendation was not adopted in the Bill.

Provisions in the Ombudsmen Act are sufficient to protect the Office of the Ombudsman's ability to conduct investigations without resorting to wholesale exclusion from the Privacy Act.

Codes of practice

The Council lauds Parliament for its foresight in giving the Privacy Commissioner tools to enact policies to adjust all of government privacy standards without requiring another act of Parliament. However, the Bill as currently written allows the Privacy Commissioner to strengthen *or weaken* the rights established by the Act. The Council opposes this unreasonable attack on the rights of New Zealanders.

The Council recommends:

- Strike "less stringent" from clause 35(2)(a)(i) and from 36(2)(a)(i); and
- strike 43(1)(a) and 43(2).

Refer to GDPR

Amend 193(2)(c)(ii) to refer to the GDPR not the expired EU Data Protection Directive.